Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2023–2024

36 239 Voorstel voor een Verordening betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordening (EU) 2019/1020

H

BRIEF VAN VICEVOORZITTER ŠEFČOVIČ VAN DE EUROPESE COMMISSIE EN LID BRETON

Aan de voorzitter van de vaste commissie voor Justitie en Veiligheid

Cc: Aan de Voorzitter van de Eerste Kamer der Staten-Generaal

Brussel, 25 september 2023

De Commissie dankt de Eerste Kamer voor haar tweede brief over het voorstel voor een verordening van het Europees Parlement en de Raad betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordening (EU) 2019/1020 (COM(2022)454 final).

Het voorstel van de Commissie («de CRA») wordt een belangrijke mijlpaal bij de verbetering van de Europese cyberbeveiliging op alle gebieden. Het heeft tot doel gemeenschappelijke verplichte eisen voor de cyberbeveiliging van producten met digitale elementen vast te stellen, gedurende hun hele levenscyclus.

Voor het antwoord op de meer technische vragen en opmerkingen in de brief verwijst de Commissie naar de bijlage.

De Europese Commissie hoopt dat zij met de toelichting in dit antwoord voldoende is ingegaan op de door de Eerste Kamer aan de orde gestelde punten en zij kijkt ernaar uit de politieke dialoog in de toekomst voort te zetten.

De uitvoerend Vicevoorzitter,
M. Šefčovič

Lid van de Commissie,
T. Breton

kst-36239-H
ISSN 0921 - 7371
's-Gravenhage 2023

BIJLAGE

Vrije en open source software

De Commissie is vastbesloten het opensource-ecosysteem te ondersteunen en onderkent ten volle de voordelen van het opensource-ecosysteem voor innovatie en de economie als geheel. Met betrekking tot de vragen van de leden van de Eerste Kamer over de reden waarom de Commissie niet heeft gekozen voor een inkadering die gebaseerd is op het doel waarmee een product met digitale elementen is ontwikkeld, herhaalt de Commissie dat de uitsluiting van niet-commerciële opensource-software de algemene aanpak van het zogenaamde «nieuwe wetgevingskader»[1] volgt.

Conform het nieuwe wetgevingskader en de bijbehorende richtlijnen in de Blauwe Gids van 2022 voor de uitvoering van de productvoorschriften van de EU[2] hangt de beoordeling of een product wordt geleverd in het kader van een handelsactiviteit af van de vraag of het product in een zakelijke context wordt geleverd. De Commissie is van mening dat dat per geval moet worden beoordeeld. Bij die beoordeling moeten verschillende factoren in acht worden genomen, waaronder die van overweging 10 van het voorstel[3], om de «zakelijke intentie» van de fabrikant van het product aan te tonen.

Zoals vermeld in haar antwoord op de eerste brief van de Eerste Kamer over dit voorstel, is de Commissie van mening dat de CRA moet bepalen welke regels van toepassing zijn op het beschikbaar stellen van producten met digitale elementen. Dit betreft een verduidelijking van de criteria voor de definitie van de levering van opensourceproducten in het kader van een handelsactiviteit, zonder dat alle gevallen uitputtend worden beschreven. Die bepalingen kunnen na de goedkeuring van het voorstel verder met relevante richtsnoeren worden aangevuld.

Duidelijkheid van de eisen

De Commissie analyseert nauwgezet de feedback van belanghebbenden na de goedkeuring van het CRA-voorstel. Dit omvat feedback van de vrije en opensource-softwaregemeenschap.

De CRA is evenredig en risicogebaseerd. Het voorstel is alleen van toepassing op het verstrekken van een product met digitale elementen in het kader van een handelsactiviteit, en essentiële cyberbeveiligingsvereisten moeten worden toegepast met inachtneming van de resultaten van de risicobeoordeling en de eigenschappen van het product. Bovendien

---

[1] Het nieuwe wetgevingskader bestaat uit Verordening (EG) nr. 765/2008 tot vaststelling van de eisen inzake accreditatie en markttoezicht betreffende het verhandelen van producten; Besluit nr. 768/2008/EG betreffende een gemeenschappelijk kader voor het verhandelen van producten en betreffende een gemeenschappelijk kader voor het verhandelen van producten en Verordening (EU) 2019/1020 betreffende markttoezicht en conformiteit van producten.

[2] PB C 272 van 26.7.2016, blz. 1, beschikbaar op: https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:52016XC0726(02).

[3] Overweging 10 van de CRA luidt: 10) Om innovatie of onderzoek niet in de weg te staan, mag vrije en opensourcesoftware die buiten het kader van een handelsactiviteit wordt ontwikkeld of geleverd, niet onder deze verordening vallen. Dit geldt met name voor software, met inbegrip van de broncode en gewijzigde versies ervan, die openlijk gedeeld en vrij toegankelijk, bruikbaar, veranderbaar en herdistribueerbaar is. In de context van software omvat een handelsactiviteit mogelijk niet alleen het in rekening brengen van een prijs voor een product, maar ook het in rekening brengen van een prijs voor technische ondersteuningsdiensten, het aanbieden van een softwareplatform waarmee de fabrikant andere diensten te gelde maakt, of het gebruik van persoonsgegevens voor andere redenen dan uitsluitend de verbetering van de beveiliging, compatibiliteit of interoperabiliteit van de software.

zou slechts een klein deel van de producten aan een verplichte beoordeling door derden worden onderworpen (categorie producten van klasse II zoals vermeld in bijlage III bij de voorgestelde verordening).

De Commissie wijst erop dat de CRA weliswaar nalevingskosten met zich mee zou brengen voor de entiteiten die producten in de handel brengen, maar ook aanzienlijke voordelen zou opleveren door het cyberbeveiligingsniveau van die producten te verhogen en de vereisten te harmoniseren. De Commissie treft voorbereidingen om fabrikanten, met name kleine en micro-ondernemingen, te ondersteunen bij de uitvoering van de CRA, onder meer door middel van financiële steunprogramma's en richtsnoeren. Zij is ook bereid om verdere maatregelen te onderzoeken die de lasten voor kleine en micro-ondernemingen kunnen verlichten zonder de algemene cyberbeveiligingsdoelstellingen van de CRA te schaden.

De uitvoering van de essentiële cyberbeveiligingsvereisten waarvoor de fabrikanten de conformiteit moeten aantonen overeenkomstig de CRA, wordt middels geharmoniseerde normen nader bepaald en gefaciliteerd. Die normen worden ontwikkeld op basis van een verzoek van de Commissie voor de toepassing van de CRA. De Commissie vertrouwt erop dat de nodige normen van kracht zijn als de CRA van toepassing wordt, aangezien de voorbereidende werkzaamheden inzake normen reeds van start zijn gegaan en voor de CRA een overgangsperiode (van 24 maanden) is voorgesteld.

De vaststelling van geharmoniseerde normen door de Europese normalisatieorganisaties betekent niet dat geheel nieuwe normen moeten worden opgesteld. Een bestaande (internationale) norm kan worden aangewezen als geharmoniseerde norm voor het vermoeden van overeenstemming met de essentiële vereisten krachtens Uniewetgeving. De normen worden ontwikkeld met inachtneming van bestaande internationale normen en alle andere relevante normen die zijn ontwikkeld, met inbegrip van normen op basis van andere Uniewetgeving betreffende producten, zoals de gedelegeerde handeling van de richtlijn radioapparatuur. De lopende voorbereidende werkzaamheden voorafgaand aan het normalisatieverzoek voor de CRA omvatten een inventarisatie en een kloofanalyse om te bepalen in hoeverre de bestaande internationale en Europese normen de essentiële vereisten van de CRA dekken.

Levensduur

Krachtens de CRA zijn fabrikanten verplicht om in hun producten ontdekte kwetsbaarheden aan te pakken gedurende een periode van vijf jaar nadat zij in de handel zijn gebracht. Gezien het voorgestelde brede toepassingsgebied van de CRA is een periode van vijf jaar gekozen als een redelijke gemiddelde termijn. Dit biedt ook rechtszekerheid en is verder in overeenstemming met de resultaten van de raadplegingen van belanghebbenden tijdens de voorbereiding van het CRA-voorstel. Deze vijf jaar vormen de minimumperiode waarin fabrikanten verplicht zouden zijn om de aanpak van kwetsbaarheden te verzekeren. Er wordt ook verwacht dat er marktprikkels voor fabrikanten zullen zijn om zelfs na deze termijn voor veiligheidsondersteuning te zorgen.

Sommige producten kunnen een langere verwachte levensduur hebben, maar de termijn van vijf jaar is al aan de lange kant voor verscheidene onder de CRA vallende producten. Zo is uit een enquête in 2018 onder fabrikanten van smartphones gebleken dat 14 van de 19 fabrikanten

minder dan drie jaar beveiligingsupdates verstrekken[4]. Verplichte beveiligingsupdates voor langer dan vijf jaar kunnen nadelig zijn voor de risicobereidheid van fabrikanten en met name van het mkb en start-ups: als fabrikanten een nieuw product in de handel brengen, weten zij niet of dit product commercieel succesvol wordt.

Kunstmatige intelligentie

De Commissie acht het van essentieel belang om de cyberweerbaarheid van alle producten met digitale elementen, inclusief systemen op het gebied van kunstmatige intelligentie (AI), te waarborgen, aangezien ieder connecteerbaar product kan worden gehackt. In de regel moeten fabrikanten van onder de CRA vallende AI-systemen aan de verplichtingen uit hoofde van de verordening voldoen.

De CRA legt een specifieke wisselwerking vast voor AI-systemen met een hoog risico die onder de voorgestelde AI-verordening vallen (COM (2021) 206 final). De AI-verordening (artikel 15) bevat cyberbeveiligingsvereisten voor AI-systemen met een hoog risico die in de handel worden gebracht of worden aangeboden. Deze wisselwerking tussen de CRA en de AI-verordening is geregeld in artikel 8 van de CRA en kan als volgt worden samengevat: producten met digitale elementen die overeenkomstig de AI-verordening als AI-systemen met een hoog risico worden aangemerkt en binnen het toepassingsgebied van de CRA vallen, moeten aan de essentiële eisen van de CRA voldoen. Indien die AI-systemen met een hoog risico voldoen aan de essentiële eisen van de CRA moeten ze in overeenstemming worden geacht met de in de AI-verordening vastgestelde eisen inzake cyberbeveiliging, voor zover die eisen onder de krachtens de voorgestelde CRA uitgevaardigde EU-conformiteitsverklaring of delen daarvan vallen.

In de regel zijn de desbetreffende bepalingen van de AI-verordening van toepassing ten aanzien van de conformiteitsbeoordelingsprocedures met betrekking tot de essentiële cyberbeveiligingsvereisten van een product met digitale elementen dat onder de voorgestelde CRA valt en als AI-systeem met een hoog risico is aangemerkt.

Voor kritieke producten met digitale elementen die als AI-systemen met een hoog risico worden aangemerkt en waarvoor het door de CRA vereiste zekerheidsniveau hoger is dan bij de AI-verordening is vereist, zouden bij uitzondering de conformiteitsbeoordelingsregels van de voorgestelde CRA van toepassing zijn naast die van de AI-verordening.

[4] Euroconsumers (2021) «Hackable home project: Euroconsumers unveils worrying results for smart device owners», te vinden op: https://assets.ctfassets.net/iapmw8ie3ije/1YOk8JU1LogUJFn898wLH1/7302188d91713d1b007811c4e8343c84/Hackable_home_press_release.pdf.